## REMARKS/ARGUMENTS

We have canceled claims 21-30, 32-37, and 42; and we have added claims 43-47 of which claim 47 is a new independent claims and the others are dependent claims. Upon entering these amendments claims 1-20, 31, 38-41 and 43-47 will be pending in this application.

The examiner rejected claims 1-4, 9-11, 14-16, 21-22, 26-27, 31, 33, 37-38, 41, and 42 under 35 U.S.C. §102(a) as anticipated by Stallings. But we disagree that Stallings does in fact disclose all of the elements required by claim 1 as argued by the examiner.

The purpose of the Stallings protocol is to distribute one-time session keys that Initiator A and Responder B can use in exchanges with each other. In contrast, the claimed invention relates to a way of enhancing protection of encrypted material without increasing the burden on client to remember a big password. As a result there are some fundamental differences between what Stallings discloses and what is required by original claim 1.

For example, the examiner equates nonce $N_1$, which is generated by the key Distribution Center (KDC), with a first secret. Though it might be true that an opponent would find it difficult to guess the nonce $N_1$, claim 1 requires something different from that, namely, claim 1 recites that "the client information is derived such that the server can not feasibly determine the first secret." Not only is nonce $N_1$ not a first secret, the client information that is supposedly derived from it, namely, Request $\|$ $N_1$, does not in any way hide the nonce $N_1$ from the KDC. Indeed, it is essential that the KDC be able to determine N1 because the KDC must return the nonce along with a one-time session key to initiator A. Fig. 9 of Stallings indicates that the nonce N1 is not concealed from the KDC. So, contrary to what the examiner argues Stallings does not disclose that "the client information is derived such that the server can not feasibly determine the first secret," as required by original claim 1.

In addition, the examiner characterizes nonce $N_2$ as an encrypted secret. But again that characterization is inappropriate. Nonce $N_2$ is not an encrypted secret that is stored by Responder B. On the contrary, Responder B generates $N_2$ and then encrypts it with the session key $K_s$ that it just received from Initiator A. Since Responder B does not know session key prior

to receiving it from Initiator A, it is unable to even calculate the encrypted version of nonce $N_2$ until it receives the session key.

Thus, we submit that the examiner's rejection of original claim1 was not supported by the Stallings reference and that claim 1 was patentable over that reference. Original claim 38 was patentable over Stallings reference for similar reasons.

In this response, however, we have refocused claim 1 and claim 38 by adding reference to the nature of the exchange that takes place between the client and the server to produce the decryption key. More specifically, amended claim 1 now recites:

> ...implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the sever secret, wherein the protocol is implemented so that the client cannot feasibly determine the sever secret and the server cannot feasibly determine the client secret or the third secret

Stallings does not disclose or even suggest a client and sever implementing this feature of using a multi-party secure computation protocol to compute a third secret.

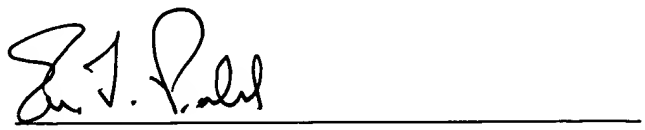
We have added similar language to amended claim 38 and to new independent claim 47.

For the reasons stated above, we believe that the claims are allowable and therefore ask the Examiner to allow them to issue.

Please apply any charges not covered, or any credits, to Deposit Account No. 08-0219.

Respectfully submitted,

Date: December 17, 2004



Eric L. Prahl
Reg. No. 32,590

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109
Telephone: (617) 526-6000
Facsimile: (617) 526-5000